Kwartalnik Nr 2/2017
ISSN 1731-62-78

BIULETYN

STOWARZYSZENIA POLALARM

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem

Członek Federacji Stowarzyszeń Naukowo-Technicznych

W numerze

Szanowne Koleżanki i Koledzy,

Okres wakacyjny nie sprzyja wytrwałej i owocnej pracy. Niemniej jednak część z nas już jest po urlopach i bardzo ciężko pracuje. Chcemy aby efekty naszej pracy były zauważalne i dostrzegalne przez innych, a tym samym chcemy aby przynosiły nam one określoną satysfakcję.

Tak powinno być z naszą pracą na rzecz Stowarzyszenia. Powinniśmy chcieć jak najwięcej rozbić dla naszego środowiska, dla bezpieczeństwa naszej ulicy, dzielnicy, województwa czy państwa. Robimy wystarczająco dużo? Każdy z nas powinien na to pytanie odpowiedzieć sobie sam, w zaciszu swoich własnych przemyśleń i refleksji. Gdyby okazało się, że ktoś z nas odpowie, że robi zbyt mało to można robić znacznie więcej. Bardzo dobrą do tego bazą jest Nasze Stowarzyszenie. Tutaj możemy się realizować, rozwijać, pracować, robić, działać we wszystkich możliwych kierunkach, obszarach i dziedzinach jakie tylko sobie wymyślimy. Od nas tak naprawdę zależy co będziemy chcieli i z jakim natężeniem robić. Nikt nam nic nie narzuca, nikt nam nic nie każe. Robimy bo chcemy coś zmienić, poprawić czy ulepszyć. Chcemy poczuć satysfakcję. To dobrze. Należy nam się odrobina satysfakcji z tego co robimy.

Róbmy więc!

Nie trzeba nic więcej. Trzeba tylko chcieć. Jesteśmy ze sobą w ramach Naszego Stowarzyszenia po to aby robić dobre i właściwe rzeczy dla branży bezpieczeństwa w Polsce.

Zabezpieczenia Nr 3 (115)/2017;

W kolejnym numerze Zabezpieczeń znajdziemy relację ze Spotkania Projektantów Niskoprądowych SPIN Extra 2017, które tym razem odbyło się w Hotelu Aquarius w Kołobrzegu w dniach 15-16 marca 2017 r. Organizatorem była firma Lockus. Wydarzenie umożliwiło podzielenie się wiedzą i nawiązanie kontaktów. Wzięło w nim udział ponad 210 uczestników: projektanci, producenci, dystrybutorzy i branżowi eksperci. Prelekcje wygłosiło 25 prelegentów, a 28 firm zaprezentowało swoje rozwiązania na stoiskach wystawienniczych. Program wydarzenia wzbogaciły dwa panele eksperckie. Prelegenci omówili standardy i dobre praktyki związane z projektowaniem bezpiecznej infrastruktury teleinformatycznej w środowisku medycznym, projektowanie współczesnych sieci komputerowych oraz praktyczne zastosowania inteligentnej analizy obrazu w projektach komercyjnych. Zaprezentowane zostały także innowacyjne techniki monitorowania, najnowsze rozwiązania z zakresu elektronicznych depozytorów kluczy i przedmiotów, nowe zasilacze do systemów zabezpieczeń, przełomowe techniki ochrony, rejestracji i archiwizacji materiału wizyjnego oraz wiele innych.

Zabezpieczenia Nr 3 (115)/2017;

Kolejny interesujący artykuł w tym numerze Zabezpieczeń to wystąpienie dr Andrzeja Wójcika na temat podstaw przeprowadzania audytu. Autor wskazuje, że audyt bezpieczeństwa obiektu to całokształt przedsięwzięć, których celem jest uzyskanie pełnych informacji o stanie bezpieczeństwa jednostki organizacyjnej, które w konsekwencji umożliwia podniesienie poziomu bezpieczeństwa we wszystkich strefach działalności organizacji oraz stworzenie warunków skutecznego reagowania na potencjalne zagrożenia i sytuacje kryzysowe. Według autora audytor to ten, kto ocenia, przeprowadza kontrolę, dokonuje przeglądu, sporządza raport – również w każdej innej branży. Ze względu na wąskie specjalizacje audytorzy branżowi powinni być fachowcami w swoich dziedzinach. Autor ponadto zwraca uwagę, że realizacja pojedynczego zadania audytowego ma dostarczyć informacji na temat poprawności przestrzegania zasad i norm dotyczących bezpieczeństwa w trakcie realizowanych procesów objętych audytem.

ABI EXPERT Nr 2 (3) kwiecień-czerwiec 2017;

W części dotyczącej aktualności w bieżącym numerze ABI EXPERT znajdziemy relację z Forum Administratorów Bezpieczeństwa Informacji, które odbyło się a dniach 3-4 kwietnia 2017 r. w hotelu Sobienie Królewski k. Warszawy. Celem spotkania było przygotowanie do wdrożenia unijnych przepisów ogólnego rozporządzenia o ochronie danych osobowych (rodo), które zacznie być stosowane od 25 maja 2018 r.

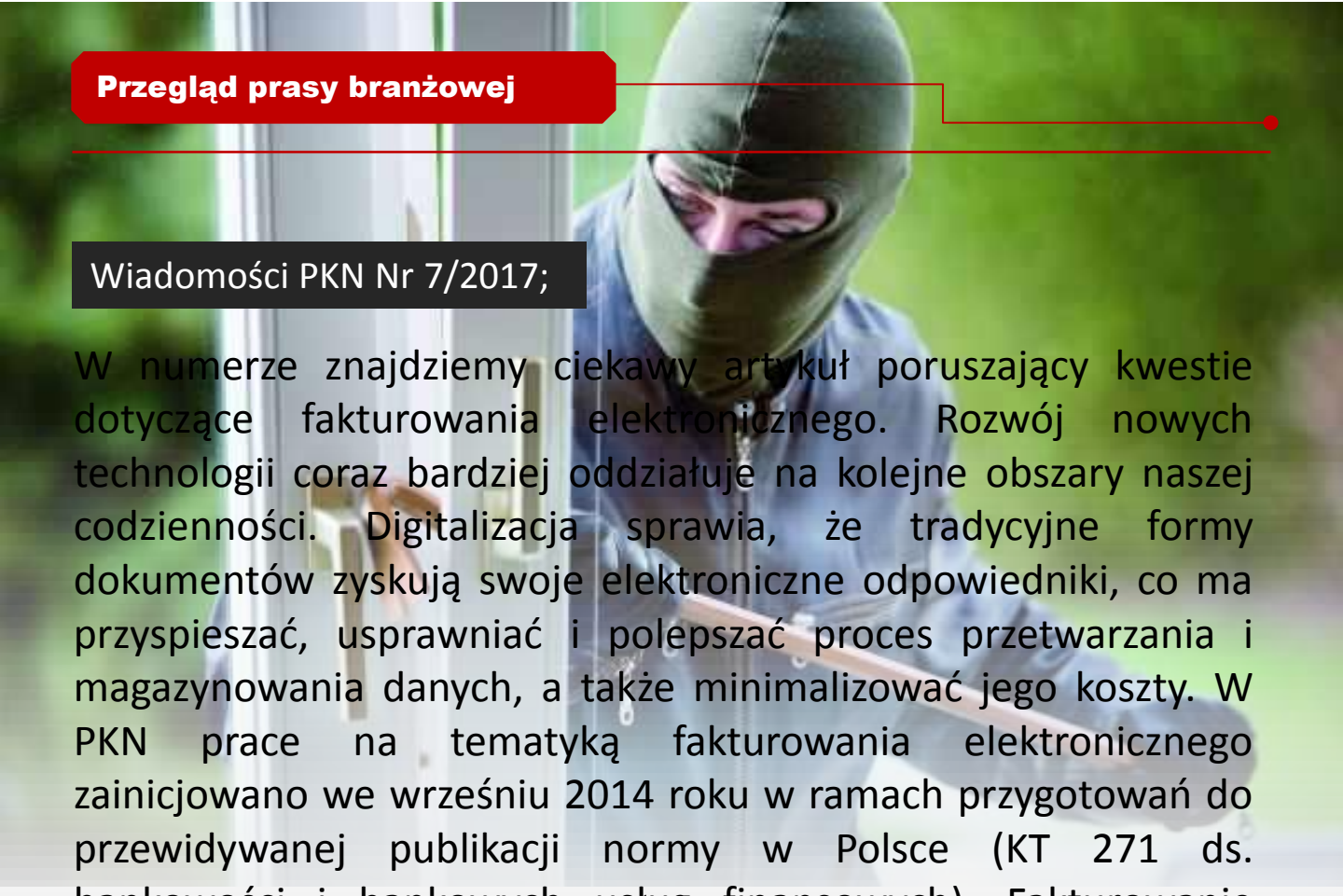
Uczestnicy konferencji dowiedzieli się: jak wyznaczyć IOD na tle wytycznych Grupy Roboczej art. 29, czym jest prawo do przenoszenia danych i jakie problemy praktyczne może sprawiać jego realizacja, jak realizować prawo do bycia zapomnianym oraz obowiązek zgłaszania naruszeń ochrony danych, jak przygotować dokumentację przetwarzania danych osobowych. Główny nacisk podczas poszczególnych prelekcji został położony na praktyczny aspekt realizacji przepisów rodo.

ABI EXPERT Nr 2 (3) kwiecień-czerwiec 2017;

Kolejnym ciekawym artykułem jaki znajdziemy w numerze ABI EXPERT jest wystąpienie Pana Jacka Orłowskiego pod tytułem Tworzenie regulaminów poczty elektronicznej. Artykuł o tyle ciekawy co istotny ze względu na dość permanentny kontakt nas wszystkich z problemem. Każdy z nas korzysta z poczty elektronicznej. Każdy więc powinien wiedzieć co nie co na ten temat. W artykule zostały przedstawione najważniejsze zagadnienia w zakresie kompetencji zarówno z punktu widzenia pracodawcy, jak i pracownika, które powinny zostać jasno określone dla dobra obu stron. Na tym tle głównym problemem okazuje się nieznajomość prawa i zasad korzystania z poczty służbowej. Po lekturze artykułu jedno jest pewne, brak przejrzystego określenia odnotowanych kompetencji generuje spory między pracownikiem a pracodawcą. By uniknąć kłopotów i ustrzec się ewentualnych roszczeń z tytułu naruszenia prywatności postrzeganej jako dobra osobiste pracowników, wielu pracodawców wprowadza przejrzyste zasady korzystania ze służbowej skrzynki elektronicznej. W ocenie autora najodpowiedniejszym dokumentem, który reguluje tego typu kwestie jest regulamin korzystania z poczty elektronicznej. Autor w artykule podaje bardzo szczegółowo w jaki sposób tego typu regulamin powinien zostać opracowany i co powinien zawierać. W wyniku lektury można śmiało rozpocząć prace na tworzeniem tego typu dokumentu w swojej organizacji. Jasne wytyczne jakie znajdziemy w artykule pozwolą w sposób skuteczny wykonać określony dokument i wprowadzić w organizacji kolejną regulację, która pozwoli uniknąć kłopotów.

Biuletyn Informacyjny Federacji Stowarzyszeń Naukowo-Technicznych Nr 4-5/2-2017;

W numerze znajdziemy relację z organizowanej już po raz piąty 25 kwietnia br. w gmachu Związku Rzemiosła Polskiego w Warszawie Konferencji Naukowo-Technicznej z cyklu „Łączy nas kształcenie zawodowe”. Patronat nad konferencją sprawowała Minister Edukacji Narodowej – Anna Zalewska. Celem zorganizowanej wspólnie przez FSNT-NOT i ZRP konferencji było dostosowanie oferty edukacyjnej do potrzeb rynku pracy, zadbanie o nowoczesne programy nauczania oraz podwyższanie jakości kształcenia zawodowego. Obydwa stowarzyszenia są zaangażowane w kształcenie dualne (łączenie praktyki z teorią szkolną), uczestniczą w procesie tworzenia treści kształcenia zawodowego, realizują je, są zawodowymi egzaminatorami.

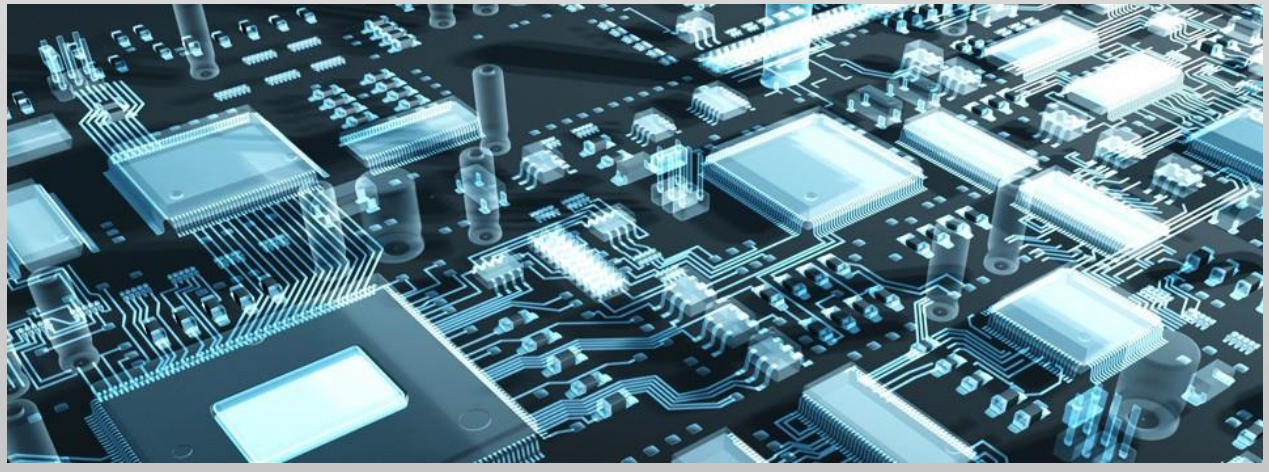


Wiadomości PKN Nr 7/2017;

W numerze znajdziemy ciekawy artykuł poruszający kwestie dotyczące fakturowania elektronicznego. Rozwój nowych technologii coraz bardziej oddziałuje na kolejne obszary naszej codzienności. Digitalizacja sprawia, że tradycyjne formy dokumentów zyskują swoje elektroniczne odpowiedniki, co ma przyspieszać, usprawniać i polepszać proces przetwarzania i magazynowania danych, a także minimalizować jego koszty. W PKN prace na tematyką fakturowania elektronicznego zainicjowano we wrześniu 2014 roku w ramach przygotowań do przewidywanej publikacji normy w Polsce (KT 271 ds. bankowości i bankowych usług finansowych). Fakturowanie elektroniczne jako metoda wsparcia handlu i jego rozliczeń jest stosowane przez wiele przedsiębiorstw komercyjnych na całym świecie. Aby ujednolicić kwestie przygotowywania i wysyłania faktury w formie elektronicznej należy opracować normę, która ujednolici i usystematyzuje kwestie fakturowania elektronicznego. Norma ustanawia semantyczny model danych części głównej faktury elektronicznej. Zawiera on tylko istotne elementy informacyjne niezbędne do zapewnienia zgodności prawnej oraz podatkowej oraz umożliwiające interoperacyjność w handlu transgranicznym, ponadsektorowym i krajowym.

Ochrona Mienia i Informacji Nr 3/2017;

W numerze znajdziemy relację z walnego zgromadzenie oraz obchodów 25-lecia Polskiego Związku Pracodawców Ochrona, które odbyło się 6 czerwca w Hotelu Warszawianka w Jachrance. Przedmiotem dyskusji była sytuacja w branży ochrony po zmianach legislacyjnych dotyczących rynku pracy oraz czekające ją wyzwania. Udział w wydarzeniu wzięli między innymi przedstawiciele Głównego Inspektoratu Pracy, Wydziału Nadzoru nad SUFO Biura Prewencji Komendy Głównej Policji, Federacji Przedsiębiorców Polskich oraz szeregu wystawców – firm oferujących produkty i usługi dedykowane sektorowi ochrony, którzy zaprezentowali nowości i rozwiązania technologiczne. Polski Związek Pracodawców Ochrona to dobrowolna, samorządna i niezależna organizacja skupiająca wiodących pracodawców branży bezpieczeństwa w Polsce. Reprezentuje firmy branży, zatrudniające ponad 100 tysięcy pracowników.



Ochrona Mienia i Informacji Nr 3/2017;

Ponadto w numerze znajdziemy artykuł dotyczący integracji systemów monitoringu i kontroli dostępu w ramach BMS. Jak pisze autor w nowoczesnych systemach budynku inteligentnego integrujących poszczególne instalacje istotną rolę ogrywa proces przesyłu danych. Stąd też informacje są wymieniane ringowo w ramach poszczególnych rozdzielni automatyki i gwieździście w ramach interfejsów sterowania. Proces przesyłu informacji niejednokrotnie bazuje na magistrali komunikacji szeregowej. Jej istotną cechą jest struktura rozproszona, którą można przewidzieć już na etapie projektowania okablowania. Tym samym można rekonfigurować i rozszerzać system na każdym etapie użytkowania obiektu

Przywołując definicję, klarownie przywołaną przez Rządowe Centrum Bezpieczeństwa, „Infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia, instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa.” Definicja taka w swoim założeniu jest bardzo szeroka a jednocześnie dość precyzyjna i dokładna. Obejmuje ona systemy zaopatrzenia w energię, surowce energetyczne i paliwa, zaopatrzenia w żywność, w wodę, systemy: łączności, sieci teleinformatycznych, finansowe, ochrony zdrowia, transportowe, ratownicze oraz produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych. Definicja taka w identycznym lub nieco zmodyfikowanym brzmieniu przytaczana jest przez znaczącą większość osób zajmujących się infrastrukturą krytyczną. Definicja ta została przyjęta i zaakceptowana przez osoby zajmujące się na co dzień i zarządzające kwestiami bezpieczeństwa właśnie w obiektach zaszeregowanych do grupy obiektów infrastruktury krytycznej.
Cytując dalej za RCB, ochrona infrastruktury krytycznej polega na: ochronie fizycznej, ochronie technicznej, ochronie osobowej, ochronie teleinformatycznej, ochronie prawnej oraz na stosowaniu tworzeniu i wykorzystywaniu planów odtwarzania. Podobnie jak w poprzednim akapicie, nie sposób nie zgodzić się z taką klasyfikacją RCB. Definicja ta wyczerpuje wszelkie działania mające na celu właściwe zabezpieczenie dowolnego obiektu, który z jakichś powodów chcemy chronić. Wszelkie organizacje pragnące zapisać w swoich dokumentach normatywnych potrzebę ochrony swoich obiektów powinny korzystać z tej definicji.

Inni specjaliści zagadnienia podają nieco prostszy podział zagrożeń infrastruktury krytycznej. Dzielą je na; zagrożenia celowe, czyli stanowiące celowe działanie człowieka oraz na zagrożenia niezamierzone, czyli błędy konstrukcyjne lub powodowane niewłaściwą eksploatacją urządzeń i instalacji.

Wszystkie wskazane wyżej zagrożenia są zjawiskami bardzo realnymi, wymagającymi ciągłego monitorowania i przeciwdziałania. Zachodzące w Europie i na Świecie zmiany społeczno-polityczne powodują, że indywidualne rodzaje zagrożeń okresowo aktywują się bardziej. Skupiając na sobie zainteresowanie społeczeństw i działania służb odpowiedzialnych za przeciwdziałanie tym, a nie innym zagrożeniom. Ważne jest jednak aby pamiętać, że sytuacja, w której dany typ zagrożenia okresowo nie jest dolegliwy, nie jest zwykle sytuacją stałą nie wymagającą jego monitorowania. Albowiem doświadczenie uczy, że okresowa „cisza" świadczy często o „utajonej" modyfikacji sposobów lub formy działania, a nie o zaniku takiego lub innego zagrożenia. Z tego względu monitorowanie zagrożeń i ciągła analiza zmian charakterystyki ich powstawania i przebiegu jest procesem niezbędnym i niestety ciągłym. Wszelkie działania w zakresie zapewnienia bezpieczeństwa tego typu obiektów powinna skupiać się w głównej mierze na zapewnieniu monitorowania określonych grup zagrożeń i weryfikowania poziomu ich występowania. Następnie określone działania zaradcze powinny być dopasowywane do odpowiedniego poziomu zagrożeń.

Dokładniejsza analiza wskazanych wcześniej zagrożeń opisana została przez wielu ekspertów i dla osób interesujących się tym zagadnieniem, jest mniej lub bardziej znana powszechnie. Ja natomiast chciałbym zwrócić uwagę na dwa rodzaje zagrożeń, które niezbyt często pojawiają się w analizach ekspertów, co może wskazywać na ich nie dostrzeganie lub na ich lekceważenie. Jak wynika z analizy tego co wcześniej został napisanie pomijanie określonych zagrożeń, niedostrzeganie ich, niewidzenie ich przy budowaniu systemów bezpieczeństwa może mieć opłakane czy wręcz tragiczne skutki dla organizacji. Nie wolno przy analizie czy później doborze odpowiednich systemów zabezpieczeń pozwolić sobie na nie branie pod uwagę określonych realnych i występujących zagrożeń. Brak reakcji na określone zagrożenie powoduje, że tym obszarze organizacja staje się bezbronna i nie może odeprzeć określonego niesprzyjającego działania na swoje zasoby. Taka sytuacja skutkować będzie realną stratą na zasobach organizacji.

Pierwsze z nich ma charakter ogólnoświatowy i związane jest z lawinowo narastającym postępem technologicznym. Większość specjalistów zajmujących się na co dzień bezpieczeństwem fizycznym, jeszcze całkiem niedawno, systemy służące wykryciu i zapobieganiu sytuacjom niepożądanym dzieliła na systemy włamania i napadu, systemy dozorowe CCTV oraz systemy kontroli dostępu. Bardzo podobnie postrzegali je użytkownicy czy zarządzający ochranianymi obiektami.

Tak określone systemy oczywiście pozwalały na realizację kanonów zabezpieczania, czyli przede wszystkim na ograniczenie fizycznego dostępu do obiektów i instalacji osobom do tego nie uprawnionym. Pozwalały też na wykrycie zaistnienia ewentualnego wtargnięcia intruzów oraz na obserwację obiektu lub instalacji i ujawnienie działań realizowanych przeciw bezpieczeństwu osób lub mienia. Detektory każdego z takich systemów wysyłały do swoich central alarmowych, czy stacji zarządzających a za ich pośrednictwem do centrum monitorowania zdarzeń, określoną ilość informacji. Oprócz informacji o zdarzeniu alarmowym sygnalizowały między innymi załączenie, rozłączenie awarię, sabotaż, itp. W przypadku systemów dozorowych CCTV przesyłały oczywiście także informacje odpowiadające zdarzeniom obserwowanym przez indywidualną kamerę. W sytuacji modelowej, zwykle choć nie zawsze stosowanej, informacje te były analizowane przez operatora systemu zabezpieczenia. Wnioski z zaobserwowanych zdarzeń przekładały się na jego reakcję, skutkując interwencją mającą na celu przeciwdziałanie zaistniałej sytuacji niepożądanej.

Powyżej opisany model procesu nadzoru systemów zabezpieczenia przez operatora wynika wprost z wymogów w zakresie bezpieczeństwa oraz ze zdrowego rozsądku. Nie jest on jednak wymogiem formalnym i nikt organizacji nie może zmusić do monitorowania swoich systemów bezpieczeństwa. Można potkać się z obiektami, na których wszystkie alarmy pochodzące z systemów alarmowych są jedynie rejestrowane i analizowane po czasie wystąpienia zdarzenia.

Logika bezpieczeństwa nie jest zgodna z taką sytuacją i nie przyjmuje tego typu argumentacji do praktycznego wykorzystania. Jak można zaakceptować sytuację kiedy buduje się złożony system zabezpieczenia technicznego, a następnie nikt nie analizuje sygnałów wysyłanych przez ten system i nie podejmuje na bieżąco działań zaradczych czy przeciwdziałających.

Percepcja operatora pozwala na obserwację ograniczonej ilości systemów. Wyzwaniem dla niego są między innymi różnice technologiczne systemów, z których każdy może pochodzić od innego producenta i każdy musi zwykle być obsługiwany w inny sposób. Kolejnym nie banalnym wyzwaniem jest ilość informacji nie wskazującej na alarm, a jedynie na błędne działanie systemu tzw. fałszywe alarmy. Takie informacje operator powinien odseparować, notując jednakże ich wystąpienie, nie inicjując jednak reakcji na zdarzenie, które faktycznie nie zaistniało. Wymaga to jednak sprawdzenia i potwierdzenia, często z wykorzystaniem określonych sił i środków. Podsumowując, należy przyznać, iż model takiej organizacji systemów zabezpieczenia technicznego sprawdzał się przez lata. Szczególnie, pamiętając o fakcie, iż ceny systemów służących zabezpieczeniu technicznemu obiektów powodowały, że ilość detektorów w każdym z systemów była ograniczana, zaś w przypadku dużych obiektów zwykle można było zwiększyć liczbę operatorów.

Różnorodność i wielość systemów technicznych, mających wpływ na bezpieczeństwo indywidualnego obiektu, a także wykorzystywanie w nich elementów detekcyjnych powoduje bardzo duży dopływ informacji do stanowiska lub stanowisk operatora systemu zabezpieczenia. Powstaje więc pytanie, czy da on sobie radę z prawidłową interpretacją tak dużej ilości informacji? Wydaje się uprawnionym domniemanie, że niestety część istotnych informacji z różnych systemów pozostanie nie dostrzeżona w masie innych. Jak wiadomo możliwości percepcji człowieka nie są nieograniczone i nawet dobre wyszkolenie może poprawić tą sytuację w ograniczonym zakresie.

Kolejnym zagadnieniem, mającym bezpośredni wpływ na bezpieczeństwo obiektów są potencjalne niepokoje społeczności lokalnych lub społeczności reprezentujących skrajne przekonania np. proekologiczne, skierowane bezpośrednio przeciwko indywidualnym obiektom. Takie osoby komunikują się często i organizują swoje protesty za pośrednictwem mediów społecznościowych w Internecie. Choć oczywiście istnieją rozwiązania softwareowe pozwalające monitorować potencjalne pojawienie się tego typu zagrożeń, pytanie brzmi czy nasz wskazany wcześniej operator jest w nie wyposażony? Czy potrafi i ma czas z nich korzystać? Czy potrafi właściwie zinterpretować pozyskane w efekcie ich zastosowania informacje?

Reasumując należy stwierdzić, że wszelkie działania zmierzające z kierunku poprawy poziomu bezpieczeństwa obiektów infrastruktury krytycznej powinny być skupione na niwelowaniu określonych zagrożeń oraz na zapobieganiu skutkom ich powstawania. Nic nie dzieje się bez przyczyny i nic co się zadzieje nie pozostaje bez skutków dla organizacji. Trudno wyobrazić sobie więc sytuację kiedy to organizacja wie o określonych zagrożeniach i nie podejmuje żadnych działań aby im zapobiec czy przeciwdziałać. Organizacja określonego systemu bezpieczeństwa w obiekcie infrastruktury krytycznej powinna być nakierowana na niwelowanie określonych zidentyfikowanych zagrożeń.

Witold Strzelecki
Prezes Zarządu Stowarzyszenia POLALARM

Praca koncepcyjna związana z przygotowaniem jakiegoś projektu czy też bardziej złożonego zadania wymaga niewątpliwie pewnego wysiłku umysłowego, koncentracji i oparcia się na założonych wcześniej podstawach. Powyższe determinuje jednocześnie konieczność przygotowania sobie odpowiedniej ilości czasu na wykonanie założonej pracy. Należy również założyć, że wykonujący pracę koncepcyjną doskonale zna obszar w ramach, którego się porusza. Powinien również posiadać odpowiednie przygotowanie techniczne i merytoryczne do wykonanie koncepcji. W dzisiejszych, czasach praca koncepcyjna zastępowana jest często podawaniem wielorakich rozwiązań i przymuszeniem kierownictwa organizacji do natychmiastowego wdrożenia wybranego przez to kierownictwo rozwiązania, najczęściej w trybie zaprojektuj i wybuduj. Nie ma tu w żadnym miejscu procesu podejmowania decyzji obszaru do dyskusji na temat realnych i rzeczywistych potrzeb.

Dokonując wyboru tego, czy innego systemu zabezpieczenia technicznego mającego wspierać całość systemu bezpieczeństwa organizacji powinniśmy się kierować najczęściej atrakcyjnością ofert dostępnych na rynku i informacją o walorach danego systemu przekazywaną nam przez osoby zajmujące się sprzedażą i marketingiem. Niemniej jednak powinniśmy jednak brać przede wszystkim pod uwagę rzeczywiste potrzeby w zakresie bezpieczeństwa naszej organizacji.

Ponadto wybór ten najczęściej obwarowany jest zapisami polityk zakupowych naszej organizacji oraz obowiązującymi w tym zakresie przepisami prawa. Etap prac analitycznych i koncepcyjnych jest zatem bardzo często pomijany i w praktyce koncepcja zabezpieczenia budowana jest na wybranym, zainstalowanym i wdrożonym systemie co powoduje jej znaczne ograniczenie – zazwyczaj do możliwości tegoż systemu, który już mamy. Trudno to z punktu widzenia gospodarza systemów bezpieczeństwa negować, gdyż musi on opierać się o realia z jakimi musi na co dzień pracować.

Decyzja o wydatkowaniu środków na konkretne zabezpieczenia podejmowana jest przez kierownictwo organizacji, które podczas tego wyboru kieruje się atrakcyjnością cenową danego produktu, a nie jego przydatnością dla zabezpieczenia organizacji. Kierownictwo organizacji potrzebuje kompleksowej informacji od swojego menadżera odpowiedzialnego za bezpieczeństwo, o tym jakie zabezpieczenia w danym momencie potrzebne są w organizacji. Nierzadko się zdarza, że osoby odpowiedzialne za bezpieczeństwo nie posiadają wystarczającej wiedzy w zakresie poszczególnych systemów, a także środków i mocy przerobowych, aby wykonać rzetelną pracę koncepcyjną w danym zakresie. Może więc dojść do sytuacji, że kupione zostanie coś co nie dość, że nie jest potrzebne organizacji, to jeszcze nie pasuje technologicznie czy mentalnie do zorganizowanego już systemu bezpieczeństwa organizacji.

Kolejnym problemem jest premiowana, wspomniana powyżej szybkość wykonania zadania. Zwykle podstawowym kryterium jest czas realizacji wykonania systemu zabezpieczeń przy jednoczesnym zaniedbaniu analizy traktującej o tym, czy rzeczywiście akurat ten system jest niezbędny. Bardzo często w organizacji nie ma wiedzy czym dysponuje organizacja w określonym obszarze bezpieczeństwa. Sytuacja taka jest w większości przypadków akceptowana lub co najmniej traktowana z przymrużeniem oka, dopóki organizacja w skutek wadliwego działania systemu nie poniesie określonej straty.

Równie często kierownictwu organizacji wydaje się, że instalacja systemu zabezpieczenia rozwiązuje wszelkie problemy z bezpieczeństwem. Niestety tak nie jest, bowiem system choćby najbardziej złożony, inteligentny i zaawansowany musi działać w oparciu o stosowne procedury, przepisy i przy udziale personelu ochrony, a te wszystkie aspekty należy przewidzieć podczas budowania koncepcji bezpieczeństwa dla określonej organizacji. Inaczej mówiąc samo wykonanie choćby najdoskonalszego systemu zabezpieczeń technicznych nie spowoduje skutecznego zapewnienia poziomu bezpieczeństwa chronionego obiektu.

Świadome kierownictwo zleci wykonanie pracy koncepcyjnej wykwalifikowanemu personelowi pionu bezpieczeństwa organizacji, jeśli taki personel posiada. Jeśli nie, to powinno rozważyć zamówienie takiego materiału w firmie komercyjnej specjalizującej się w wykonywaniu takich usług.

Tu pojawia się niebezpieczeństwo zbyt mocnego i szerokiego skomercjalizowania opracowanej w takim trybie koncepcji. W opracowaniu koncepcji z wykorzystaniem wiedzy i doświadczenia firm komercyjnych zawsze powinien uczestniczyć niezależny ekspert reprezentujący organizację i dbający o jej interesy ekonomiczne i merytoryczne.

Tu szerokie pole do wykorzystania rzeczoznawców naszego Stowarzyszenia jako niezależnych ekspertów reprezentujących organizację w procesie tworzenia koncepcji systemów bezpieczeństwa.

Przechodząc do zawartości samej koncepcji zacznijmy od wskazania tego, czego w danej organizacji zamierzamy chronić czyli od zdefiniowania zasobów wrażliwych lub też krytycznych, jeśli będą występowały. Profesjonalny zespół ekspertów organizacji wsparty przez ekspertów zewnętrznych powinien wydobyć takie informacje od wyznaczonych przez kierownictwo organizacji pracowników, na podstawie przygotowanych wcześniej ankiet lub też wywiadu środowiskowego i wizji lokalnych, a następnie poprzeć je i uzupełnić o informacje pochodzące z własnej wiedzy i doświadczenia.

Kiedy wiadomo już jakie zasoby w organizacji będą ochronione należy zwrócić uwagę na zagrożenia jakie mogą wystąpić i wskutek wystąpienia, których organizacja w ogóle może ponieść straty. Stosunek porównawczy zasobów i zagrożeń powinien już przynajmniej w zarysie określić poziom ochrony jaki zamierzamy zastosować w instytucji. Często zdarza się bowiem, że nakłady poniesione na zabezpieczenia znacznie przekraczają wartość poniesionych strat w wyniku zaistnienia danego zagrożenia.

Proces definiowania zarówno zasobów jak i zagrożeń wymaga ścisłej współpracy pomiędzy eksperckim zespołem wykonawczym, a pracownikami organizacji, która wykonanie koncepcji zleciła. Możliwe wtedy jest zapewnienie efektywnego wykorzystania wiedzy i doświadczenia ekspertów zewnętrznych w połączeniu z doświadczeniem wiedzą pracowników, ich znajomością organizacji oraz jej wrażliwych punktów. Efektem takiego działania będzie wypracowanie optymalnego rozwiązania, w kwestii organizacji bezpieczeństwa.

Mając zdefiniowane zasoby i zagrożenia można określić pewne warunki brzegowe w zakresie wymagań dla systemów zabezpieczenia technicznego w sposób adekwatny do ustalonych wcześniej potrzeb organizacji w zakresie bezpieczeństwa. Powyższe pozwoli także, na przynajmniej wstępne oszacowanie kosztów, jakie firma będzie musiała ponieść w związku z organizacją systemu bezpieczeństwa. Oczywiście na tym etapie nie mówimy jeszcze o konkretnych rozwiązaniach, a tylko szacujemy ewentualne koszty budowy systemów bezpieczeństwa.

W przypadku kiedy na badanym terenie znajdują się już zainstalowane systemy zabezpieczenia technicznego nie mogą one zostać pominięte w pracach koncepcyjnych. Nie można budować przy okazji każdorazowej rozbudowy systemów bezpieczeństwa odrębnego systemu zabezpieczeń technicznych. Kluczowym zadaniem jest opis ich charakterystyki i ewentualnej przydatności dla nowoprojektowanego systemu bezpieczeństwa.

Bardzo istotne jest też zwrócenie uwagi na możliwość integracji istniejących systemów z planowanymi za pośrednictwem narzędzia integrującego, jeśli zamierzamy je zastosować. Charakteryzując i opisując systemy zabezpieczenia technicznego należy zwrócić uwagę także na personel, który nimi zarządza, a więc służbę ochrony.

Wykazać należy czy wszystkie czynności związane z sygnalizacjami systemów mają swoje odzwierciedlenie w odpowiednich procedurach postępowania pracowników ochrony fizycznej. Dokumentacja regulująca zakres odpowiedzialności służby ochronnej, a także pracowników których system ma chronić lub wykazanie braku takiej dokumentacji jest równie ważnym elementem części analitycznej koncepcji, co zdefiniowanie zasobów i zagrożeń.

Audyt posiadanych systemów zabezpieczeń technicznych opisany powyżej powinien kończyć się jasną dla organizacji oceną stanu bezpieczeństwa oraz rekomendacjami zespołu ekspertów, które wytyczą dalszy tryb postępowania w celu podniesienia czy też zapewnienia stanu bezpieczeństwa w danej organizacji. Audyt najczęściej traktowany jest w organizacjach jako zbędne wydatkowanie określonych środków finansowych. Organizacje nie widzą potrzeby przeprowadzania audytu jednocześnie nie posiadając w swoich strukturach wyspecjalizowanych komórek organizacyjnych odpowiedzialnych za bezpieczeństwo w organizacji. To bardzo dziwna praktyka, ale tak to na dziś wygląda na rynku zabezpieczeń technicznych.

Szczegółowo określone potrzeby organizacji w zakresie bezpieczeństwa pozwalają rozpocząć rzeczywistą prace nad przygotowaniem koncepcji zabezpieczeń technicznych poprzez przyjęcie wymaganej strategii i jej realizację. Zespół ekspertów przedstawia kierownictwu organizacji optymalne rozwiązanie lub rozwiązania, które powinno zostać zastosowane na wskazanym przez niego obszarze. Do najważniejszych elementów tej części zadania należy określenie formy i zakresu dokumentacji niezbędnej do prawidłowego funkcjonowania przedmiotowego modelu bezpieczeństwa, a więc wszelkich przepisów wewnętrznych regulujących zadania i obowiązki całego personelu biorącego udział w systemie bezpieczeństwa firmy, takie jak instrukcje ochrony obiektów, instrukcje ruchu osobowego i materiałowego, bezpiecznej eksploatacji i administracji systemami zabezpieczenia technicznego itp.

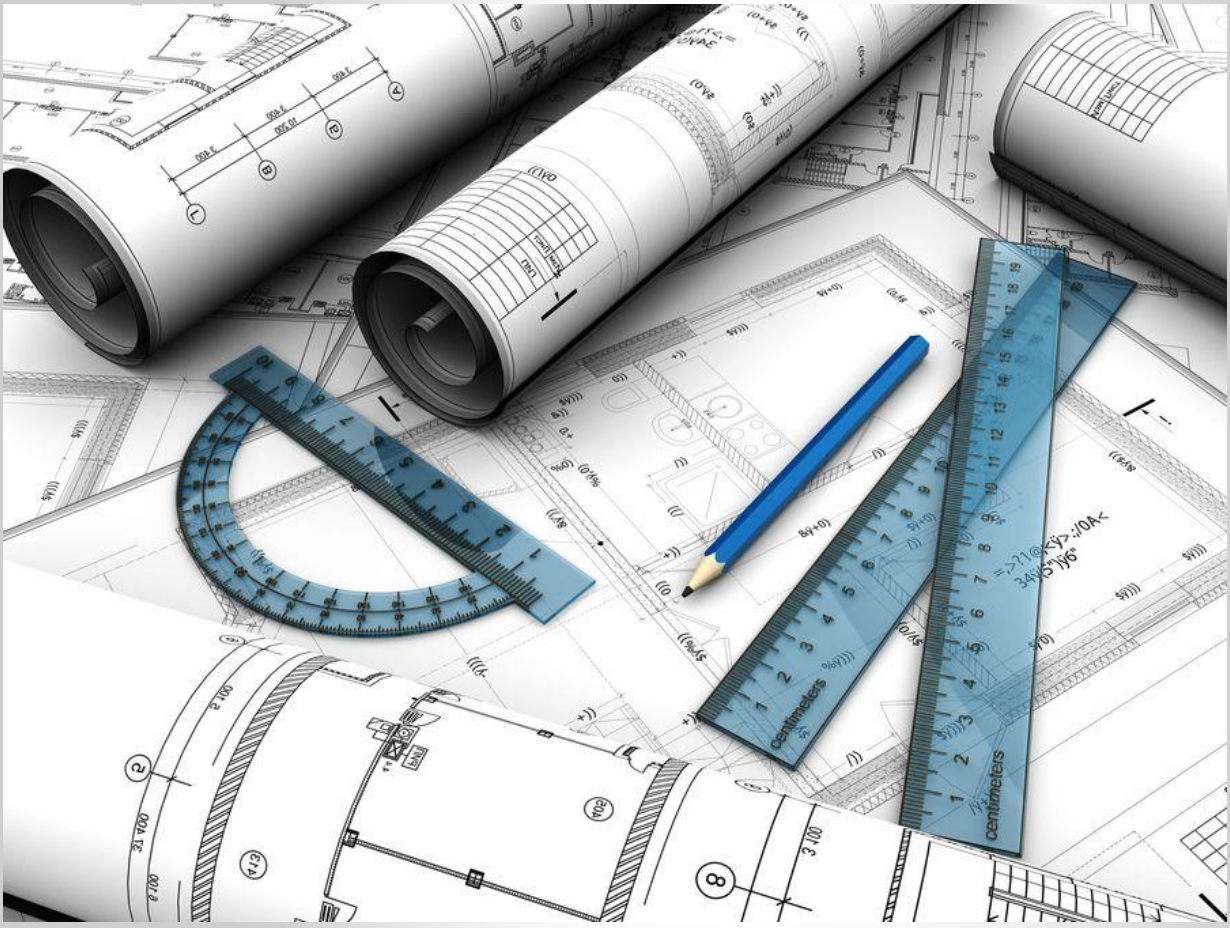
Ponadto wskazane zostaną systemy, które są niezbędne do podniesienia poziomu bezpieczeństwa wraz z szczegółowymi wymaganiami dotyczącymi ich instalacji i eksploatacji. Oczywiście koncepcja nie zawiera tych wszystkich dokumentów i nie jest rozwiązaniem wszystkich problemów organizacji w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa organizacji. Koncepcja dotyka wskazanych obszarów czy przestrzeni, wiąże je ze sobą odpowiednimi nitkami zależności, których główną osią są techniczne systemy zabezpieczeń.

Gotowy produkt jakim jest koncepcja zabezpieczenia danej organizacji powinien w swoim podsumowaniu zawierać opis sposobu wdrożenia wzorcowego modelu bezpieczeństwa wraz szacunkowym jego kosztem. Warto także zadbać o to, aby integralną częścią koncepcji był przykładowy opis przedmiotu zamówienia czy tez program funkcjonalno-użytkowy.

Oczywiście zakres opracowania koncepcji powinien być jasno określony nim zespół ekspertów przystąpi do jej opracowywania. Praktyka w tym zakresie pokazuje, że często organizacja zleca opracowanie koncepcji w bardzo wąskim, wręcz szczątkowymi zakresie, a następnie wraz z powstawaniem koncepcji rośnie apetyt organizacji na zwiększanie zakresu koncepcji w sposób wręcz nieskończony.

Odwołując się do swojego długoletniego doświadczenia w branży zabezpieczeń technicznych zdecydowanie jestem przekonany, że poświęcenie czasu i zaangażowania pewnych środków finansowych na sporządzenie koncepcji dla rozwiązań stosowanych w systemie bezpieczeństwa organizacji znacznie pomoże w określeniu jego strategii i dalszej budowie, a także późniejszej eksploatacji.

W zakresie systemów zabezpieczenia natomiast, zatwierdzona przez kierownictwo organizacji koncepcja może posłużyć jako zestaw szczegółowych wytycznych do opracowania dokładnych projektów wykonawczych poszczególnych systemów.



Biuro Usług Rzeczoznawczych i Konsultingowych

W ramach Ogólnopolskie Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **POLALARM**, które jest organizacją o charakterze naukowo-technicznym, zrzeszającą osoby zajmujące się w sposób profesjonalny zagadnieniami związanymi z technicznym zabezpieczeniem osób i mienia, kwestiami bezpieczeństwa informacji i zabezpieczania danych oraz problematyką zarządzania bezpieczeństwem funkcjonuje Biuro Usług Rzeczoznawczych i Konsultingowych (BURiK).

W dyspozycji Biura pozostaje ponad 100 przeszkolonych rzeczoznawców systemów zabezpieczających na terenie całej Polski. Rzeczoznawcy posiadają niezbędną wiedzę i uprawnienia w zakresie technicznych systemów zabezpieczeń, która pozwala realizować wszelkie prace, które swoim zakresem obejmują systemy bezpieczeństwa. Rzeczoznawcy ci działają według zasad zawartych w Uchwale Nr 20/98 Rady Krajowej Federacji Stowarzyszeń Naukowo-Technicznych w sprawie statusu rzeczoznawców oraz zasad organizacji rzeczoznawstwa stowarzyszeń naukowo-technicznych zrzeszonych w Federacji SNT NOT.

Biuro Usług Rzeczoznawczych i Konsultingowych

Specjalizacja Biura Usług Rzeczoznawczych i Konsultingowych Stowarzyszenia obejmuje zagadnienia z zakresu:

- wykonywanie audytów systemów bezpieczeństwa wskazanych obiektów;
- przeprowadzanie działań audytowych w zakresie bezpieczeństwa obiektów w ujęciu normy 27001,
- opracowywanie raportów i zaleceń do udoskonalania i przebudowywania technicznych systemów zabezpieczeń, po przeprowadzeniu odpowiedniego audytu bezpieczeństwa,
- opiniowaniu projektów systemów zarządzania bezpieczeństwem,
- opiniowaniu systemów i urządzeń technicznych służących ochronie osób i mienia,
- opracowywanie koncepcji i projektów wykonawczych ochrony obiektów i obszarów z wykorzystaniem systemów technicznego zabezpieczenia osób i mienia oraz uwzględniających aspekty organizacyjne, prawne, obowiązujące procedury i instrukcje wewnętrzne,
- reprezentowania osób prawnych i instytucji państwowych w charakterze inwestora zastępczego w obszarze bezpieczeństwa technicznego,
- upowszechnianiu informacji technicznej w zakresie pozytywnie zweryfikowanych systemów i urządzeń służących ochronie osób i mienia,
- rekomendowaniu produktów i usług w dziedzinie systemów technicznej ochrony.

Zapraszamy do współpracy z Biurem. Kontakt: artur.bogusz@polalarm.org.

SZKOLENIA W STOWARZYSZENIU POLALARM

W związku z rosnącym zainteresowaniem stosowaniem praktycznym w pracy instalatorów i projektantów elektronicznych systemów zabezpieczeń obowiązujących Norm Obronnych, Nasze Stowarzyszenie organizuje szkolenia w zakresie posługiwania się Normą Obronną, Obiekty Wojskowe, Systemy Alarmowe, NO-04-A004 arkusze od 1 do 9.
Szkolenie będzie miało na celu zapoznanie z uwarunkowaniami prawnymi, organizacyjnymi, technicznymi i praktycznymi wynikającymi z zapisów poszczególnych arkuszy Normy Obronnej. Celem szkolenia jest jak najlepsze przygotowanie osób zainteresowanych do posługiwania się zapisami Normy Obronnej w praktyce projektowej czy instalatorskiej.
W POLALARMIE prowadzone są bardzo intensywne prace mające na celu przygotowanie *„Poradnika stosowania praktycznego Norm Obronnych, Obiekty wojskowe, Systemy alarmowe serii NO-04-A004 arkusze od 1 do 9”*. Publikacja ta ma być pomocna instalatorom i projektantom w praktycznym poruszaniu się w obszarze Norm Obronnych.
Wszystkich zainteresowanych odbyciem takiego szkolenia zapraszamy do zgłaszania się do Biura Stowarzyszenia pod numer telefonu +48 503 828 424 lub pod adres email: polalarm@polalarm.com.pl.

Działalność Biura Usług Rzeczoznawczych i Konsultingowych;

Jak wszyscy pewnie zdajemy sobie sprawę w ramach działalności prowadzonej w Stowarzyszeniu POLALARM działa Biuro Usług Rzeczoznawczych i Konsultingowych (w skrócie BURiK). W założeniach Zarządu Stowarzyszenia działalność Biura powinna być w dużej mierze działalnością priorytetową naszego Stowarzyszenia. Wykonywanie audytów technicznych i fizycznych systemów bezpieczeństwa, opracowywanie prac rzeczoznawczych, wydawanie opinii, realizowanie zadań inwestora zastępczego, reprezentowanie stron w sporach w określonych instytucjach czy sądach, opracowywanie koncepcji zabezpieczeń technicznych i fizycznych, wydawanie wytycznych do praktycznego stosowanie w zakresie zabezpieczeń technicznych – to główne cele i zakres działalności Biura. W ramach Stowarzyszenia zrzeszamy rzeczoznawców i ekspertów w zakresie zabezpieczeń technicznych, bezpieczeństwa fizycznego, bezpieczeństwa informacji. Posiadamy więc wszystko co powinno umożliwiać prowadzenie tego typu działalności w sposób skuteczny i efektywny.

W ramach regulacji wprowadzonych przez Zarząd Stowarzyszenia przyjęto, że rzeczoznawca wykonujący zlecenie pozyskane przez Stowarzyszenie i przekazane mu do realizacji, odprowadzi na rzecz Stowarzyszenia odpis w wysokości 20% wartości zlecenia (dotychczas było to 30%), natomiast rzeczoznawca, który pozyskał i wykonuje zlecenie w imieniu Stowarzyszenia, odprowadzi na rzecz Stowarzyszenia odpis w wysokości 10% wartości zlecenia (dotychczas było to 15%). Wydaje się, że takie regulacje powinny powodować duże zainteresowanie korzystaniem ze współpracy z Biurem, a jednocześnie ze Stowarzyszeniem.

Niestety nie wszystkie działania Biura są zadawalające i satysfakcjonujące. Nasze działania wymagają zintensyfikowania, tak aby zaczęły przynosić Stowarzyszeniu wymierne korzyści. W innym przypadku nie tylko działalność Biura, ale i działalność Stowarzyszenia stanie pod znakiem zapytania. Niestety wymaga to zaangażowania ze strony każdego jednego rzeczoznawcy, który chce realizować prace rzeczoznawcze. W innym przypadku nie uda się poprawić efektywności działania całego Biura. Tylko wspólne działania rzeczoznawców zrzeszonych w Stowarzyszeniu i Biura jako takiego mogą przynieść wymierne efekty w prowadzonych pracach.

Rynek potrzebuje specjalistycznej wiedzy oraz niezależnej organizacji, która w sposób bezstronny może wydać opinię w określonej sprawie czy zająć stanowisko we wskazanej sytuacji. Dlaczego więc nie zbudować uwarunkowań, które pozwolą zaspokoić to naturalne zapotrzebowanie rynkowe. Wszelkie niezbędne warunki są, wystarczy tylko chwilę czasu ze strony każdego rzeczoznawcy i można będzie w ramach Biura realizować określone prace rzeczoznawcze.

Reasumując w najbliższym czasie zostaną podjęte działania na szczeblu Zarządu, które mam nadzieję usprawnią pracę Biura. Poprawione uwarunkowania funkcjonowania Biura pozwolą jeszcze skutecznie realizować działania i prace rzeczoznawcze w ramach Stowarzyszenie.

Szanowne Koleżanki i Koledzy gdyby ktoś z Was miał jakieś pytania czy wątpliwości w tym zakresie, albo chcielibyście przekazać jakieś swoje uwagi w kwestii realizacji prac rzeczoznawczych to jestem do dyspozycji pod adresem: artur.bogusz@polalarm.org. Będę zobowiązany za wszelkie uwagi i wnioski w zakresie realizacji w ramach Biura określonej działalności Stowarzyszenia. Mam nadzieję, że wspólnie uda nam się wypracować satysfakcjonujące dla wszystkich rozwiązania.

Miejsce na Twoją reklamę

POLALARM

Redaktor Naczelny Biuletynu Informacyjnego: Artur Bogusz
Redakcja: Maciej Jaszczuk, Witold Strzelecki;
Stowarzyszenie POLALARM
ul. Poleczki 40, 02-822 Warszawa
tel. +48 503 828 424, 22 626 90 31;
e-mail: polalarm@polalarm.com.pl, www.polalarm.org
Konto bankowe:
ALIOR BANK 70 2490 0005 0000 4520 4686 4115

Warszawa, lipiec2017 r.